

FedRAMP Continuous Monitoring Reporting and POA&M Template Comment Disposition and FAQ



11/27/2014



Table of Contents

1. FedRAMP Continuous Monitoring Reporting and POA&M Template Comment Disposition.....	3
2. FedRAMP Continuous Monitoring Reporting and POA&M Template FAQ.....	17

1. FEDRAMP CONTINUOUS MONITORING REPORTING AND POA&M TEMPLATE COMMENT DISPOSITION

Note: FedRAMP provided responses to substantive comments provided during the public comment period. Comments with suggested editorial changes are being considered and integrated along with other editorial changes submitted with the documents.

Comment	Response
<p>Page 10, Section 2.2, Vendor Dependent Risks, 3rd bullet</p> <p>“If a CSP contacts their vendors as required and provides evidence with their monthly deliverables of this, then a vendor dependency POA&M item is not considered past due.” - Identify the kind of evidence that is acceptable. If not, there will be a gap.</p>	<p>FedRAMP would accept a copy of emails, letters, or evidence of other forms of communication between the CSP and vendor regarding the vendor dependency.</p>
<p>This section should reiterate that the scan results analyzed for the FedRAMP Continuous Monitoring Reporting Summary should reflect the same scan configurations that were used at the time of the original authorization (i.e. authenticated, updated definitions, same policy, etc.) to ensure that remediation progress is being made for any previously identified vulnerabilities.</p>	<p>FedRAMP will consider adding this language to the document.</p>
<p>It would be beneficial to identify items that are deemed satisfactory evidence to show that a vendor dependency exists and as such the associated POA&M item is not considered past due.</p>	<p>FedRAMP would accept a copy of emails, letters, or evidence of other forms of communication between the CSP and vendor regarding the vendor dependency.</p>
<p>Additional information would be helpful in this paragraph, it is unclear if appropriate evidence/justification will required to be provided in the event of Operationally Required (OR) vulnerability. If evidence/justification is required should this information be embedded in the FedRAMP POA&M report?</p>	<p>Operationally Required justification should be provided in the deviation requests.</p>

Comment	Response
<p>2.2. Deviation Requests It is normal to have deviation requests related to unique items for each CSP that must also be analyzed. Some specifics on how AOs address these items are as follows:</p> <p>Date Adjustments: Date adjustments are not treated as deviation requests, as this does not change the fact that a POA&M item is past due for remediation if it is not corrected within the required timeframe.</p> <p>I don't see a template for the Deviation Request Form (DRF) on the FedRAMP web site. It would help to have the DRF template available there.</p> <p>Wording - maybe "certain" items. I don't think the items are necessarily unique.</p> <p>Milestone Date Change is a category for Type of Request in our Oct 2013 deviation request form (DRF). Is that category being removed from the DRF?</p>	<p>1. FedRAMP will consider adding the Deviation Request Form to the POA&M Summary Guide.</p> <p>2. FedRAMP is in the process of updating the deviation request form. At this time, we do not review date change, as they are considered late regardless of the request. Risk adjustments and vendor dependencies should be included. Deviation requests are reviewed by the FedRAMP ISSO. Once the ISSO reviews and agrees, the request is then passed to the JAB for approval.</p>
<p>Vendor Dependent Risks:</p> <p>If a CSP contacts their vendors as required and provides evidence with their monthly deliverables of this, then a vendor dependency POA&M item is not considered past due.</p> <p>Vendor Dependency is not a category for Type of Request in our Oct 2013 DRF. Is Vendor Dependent Risk being added as a checkbox for Type of Request in the DRF?</p> <p>Two paragraphs later, there's the explanation that vendor dependency POA&M items are not considered past due if actively pursued with the vendor.</p> <p>It would seem that if the CSP can't get approval for risk adjustment to moderate within 30 days, then a vendor dependent high risk item shouldn't be considered past due if the CSP shows contact with the vendor during that 30 days.</p>	<p>FedRAMP is in the process of updating the deviation request form. We will add the Vendor Dependency Category to the form.</p> <p>FedRAMP requires high vendor dependencies to be mitigated to a moderate within 30 days. If this vulnerability is not mitigated in 30 days, it is counted as past due, even if the CSP is in contact with the vendor.</p>

Comment	Response
<p>2.2.1. Approval of Deviation Requests</p> <p>Is the AO the FedRAMP ISSO or someone else? How are the DRFs provided ... via upload to MAX?</p> <p>How does a CSP receive this approval from the AO? Timeframe is very important when seeking Risk Adjustment for a High rated finding. If the approval of the DRF for risk adjustment is delayed, then the POA&M item will be considered “past due” in the next month’s POA&M.</p> <p>Categorized at highest level is only for the graphs. The tables allow categorization by the H/M, H/L, and M/L while pending approval. Since Table 3-2 explains the full set of risk levels, I see no need to have a subset of that table inserted here.</p>	<p>For an agency, the AO is generally the CIO, CISO, or DAA with the ability to grant an ATO. For a FedRAMP P-ATO, the AO is the JAB, however, the FedRAMP ISSOs and JAB TRs review the CSP's Deviation Request Form and other documentation to ensure the CSP meets requirements.</p> <p>The Deviation Request Form is either uploaded to OMB Max for CSPs with a P-ATO or provided directly to the AO for Agency ATOs. 2. Agreed. We are developing a process in working with the TRs on Deviation Requests. Deviation requests are reviewed and approved monthly as part of the continuous monitoring process.</p>
<p>3.2. Overview</p> <p>Does AO provide this text? AO makes the System Status determination, so it would seem that AO would then explain the justification for that status.</p>	<p>Yes, the AO make this determination on the overall status of the system. The POA&M summary graphs and additional information in the summary document is provided as evidence of the AO's decision.</p>
<p>What signifies approval for closure of POAM items? How does CSP know when it’s safe to move items to the “Closed POAM Items” tab?</p>	<p>The CSP should close a POA&M item before submitting the Continuous Monitoring Deliverable. Closed items are verified by the ISSOs.</p>
<p>Whenever possible, use drop down menu items for consistent and accurate data input. Examples, yes or no, submitted, pending, approved, risk levels of high, medium, low.</p>	<p>FedRAMP uses drop-downs in the POA&M sheets when possible. We also use data validation to ensure consistent data.</p>

Comment	Response
<p>Columns P-X – instead of a separate column for each type of write-up, use drop down menus to select one of 4 options: vendor dependency, risk adjustment, false positive, operational requirement. Use the subsequent columns to provide additional information about each using the same approach. This makes sorting and status easier</p>	<p>FedRAMP template in this format to make it parseable. In addition, each POA&M item may fall into multiple categories out of those 4 categories.</p>
<p>a. Line 6 are the column headings for filters. Insert lines 7 and 8, the instructions, as comments to line 6 or create a separate tab with instructions. b. Date format in line 8 doesn't match the allowed format in the cell. c. Column K – use a formula to calculate a suggested scheduled completion date based on the original detection date (col J), the original risk level (col S) for high and medium. Low is manually entered. d. Add col Z index to allow sorting to restore order to an original state e. Additional columns i. Create formulas for calculating age ii. How to validate fix – if DB or web scans need additional evidence iii. Column for document referenced for deviation request, vendor dependencies and evidence of remediation.</p>	<p>1. Based on a review of the document, FedRAMP concluded the single instruction row is sufficient instructions to complete the POA&M. 2. Date format depends on local system settings, fill in the date accordingly. Follow the format provided for the milestone columns. 3. We have implemented this feature. 4. This can be achieved by just clearing the filters. 5. We have the Deviation Request ID column. Evidence of remediation is found in the next scan. 6. Age- Date format depends on local system settings, fill in the date accordingly. Follow the format provided for the milestone columns.</p>
<p>Keep Closed POAMs with Ongoing POAMs and use col N latest status to differentiate. Create an archive Tab to move completed POAMs a year or more</p>	<p>We are moving all closed items to a separate tab.</p>

Comment	Response
<p>Comment: The needs expressed by FedRAMP in these documents for uniform policy reflects exactly our contention that such policy should be inherited from the responsible agency, in this case FedRAMP, not left for resolution by “organizations” not sharing common Tier 1 and 2 responsibilities, roles and missions with the federal agencies being supported.</p> <p>Recommendation: FedRAMP should develop formal federal cloud policies and procedures as directive baselines for each SP800-53 control (such as all xx-1) referencing or implying “organization” policies and procedures. These formal policies and procedures would then be augmented as necessary, after formal approval, by CSPs for systems/services having a FedRAMP preliminary AO. CSP systems and services authorized directly by federal agencies should then inherit corresponding agency policies and procedures in place of, or augmenting, those from FedRAMP.</p> <p>All of the referenced FedRAMP documents appear to constitute potential substantive parts of the recommended federal policies and procedures set; lacking only clear labeling as such and directives for that utilization.</p>	<p>FedRAMP does not agree. FedRAMP's requirements and policies must be flexible in order to apply to a wide variety of systems and environments.</p>
<p>It is not clear from reading this document whether the “monthly” reporting cycle will be OBE once the CDM Dashboards are in place. It would be prudent to mention that the “monthly” requirement will be replaced by the near-real-time Dashboards at some point.</p>	<p>Current FedRAMP requirements do include the use of a CDM dashboard. We may consider the use of dashboards and the integration of CDM requirements at some point in the future.</p>
<p>This is not applicable always. Scheduled Completion Dates should be based on the System Owner/Team’s decision as a lot depends upon budget/funding etc.</p>	<p>The timeline for remediation of 30 days for high and 90 days for moderate is standard in the Federal government. FedRAMP guidance provides these timelines. The CSP may schedule their completion date, but will need to meet this requirement is they wish to maintain their FedRAMP compliant ATO.</p>

Comment	Response
<p>In relation to continuous monitoring and the CDM program, continuous monitoring requires a dashboard that provides access to relevant security data and information that is updated more frequently than 30 days. Under CDM the entire network should be scanned every 72 hours and the dashboard should update every 8 hours. Access to a dashboard would allow AOs the ability to view data that is conceivably more relevant due to its age and more frequently than only monthly. Are the monthly deliverables a rollup of the detailed daily data? Is the monthly information incorporated into a dashboard?</p>	<p>The monthly deliverables provide the details of the requested data items for that month, such as POA&Ms and scans. This document is more concerned with the current operations of FedRAMP. Use of a CDM dash board is something that FedRAMP may consider in the near future.</p>
<p>There is an implication that a vulnerability corresponds to a risk; but this is not true – a POA&M most likely would have a one to many mapping to vulnerabilities and the assignment to risk has considerations beyond the simple vulnerability score (such as from the CVSS value)</p>	<p>FedRAMP is not only examining the vulnerability score of a single risk, but makes a decision based on the aggregate risk presented by the system.</p>
<p>This states that the AO knows both the actual risk posture and the reported risk posture and makes a comparative assessment. Is it meant to state that the AO ensures that the data provided is relevant to an accurate depiction of the risk posture per the AO’s needs? – if so, replace “accurately” with “appropriately”...or is it meant to state that the reported risk posture is acceptable/appropriate? – if so, remove “is accurately depicted” and add “is acceptable” at the end.</p>	<p>While the summary provides an overall look at the status of the system and possible indicators of risk, the AO, or the AO's staff should also review the monthly deliverables to ensure they have a more in-depth understanding of the system's risk posture.</p>
<p>While acceptable, the finding must still be reported in the monthly report. It just doesn't have to be reported as a past due POA&M.</p>	<p>Agree.</p>

Comment	Response
<p>Misconfigured assets are generally a leading cause of security vulnerabilities. There should be a separate graph for security misconfigurations. Vulnerability information for OS, DB, App is good but without specific misconfigurations it would be hard to know the state of the CSP security environment. It may be that the configuration scan is implicit in this but it should be explicitly called out and its own data point.</p>	<p>The goal of this document is to provide a standardized method for providing a high level summary. An AO assessing the true risk must conduct their own thorough analysis.</p>
<p>The direction FedRAMP is taking on Continuous Monitoring is concerning as it reflects a trajectory inconsistent with the path forward discussed with the industry. This document does not reflect the repeated recommendations by industry to reduce the administrative burden created by FedRAMP and rely on industry approaches for the ongoing evaluation of security controls at CSPs. The overemphasis on vulnerability scanning, misapplication of NIST guidance with respect to assigning vulnerability ratings, and the excessive associated reporting requirements illustrate a lack of alignment with leading industry practices and standards. We recommend that this version of the document be withdrawn and replaced with one that provides a sustainable approach to the ongoing evaluation of CSPs. We have provided significant input to FedRAMP on the subject of continuous monitoring and we look forward to seeing this applied in the next version of this document.</p>	<p>This document is more concerned with the current operations of FedRAMP. Comments on significant changes to the Continuous Monitoring process are out of scope for this document and should have been made in relation the "Evolution of FedRAMP Continuous Monitoring Framework" paper.</p>
<p>One of the inconsistencies experienced by the members of the industry is that agency driven common reporting and management deviates from this guidance and differs between agencies. More guidance should help normalize the treatment across all agencies.</p>	<p>This document was meant to provide guidance to help standardize Continuous Monitoring reporting of CSPs to Agencies by providing a standard template and guidance around its use.</p>

Comment	Response
<p>Centralize the reporting repositories and management functions of continuous monitoring and POAM review through the FedRAMP PMO, eliminating the need to report and negotiate with each agency in addition to the PMO. This speeds up potential adoption of cloud service across the government by providing a ‘leverage’ model that reduces agency investment of cost, time and resources required to monitor continuous monitoring for cloud systems.</p>	<p>Reporting and repositories are centralized for CSPs with P-ATOs. However, at this time, the FedRAMP PMO does not have the resources to manage the assessment and authorization of all CSPs working with Federal customers. Allowing for FedRAMP compliant Agency ATOs provides the flexibility needed for agencies to meet FedRAMP requirements.</p>
<p>For Agency ATOs: Centralize the reporting repositories and management functions of continuous monitoring and POAM review through the FedRAMP PMO, eliminating the need to report and negotiate with each agency in addition to the PMO. This speeds up potential adoption of cloud service across the government by providing a ‘leverage’ model that reduces agency investment of cost, time and resources required to monitor continuous monitoring for cloud systems.</p>	<p>Reporting and repositories are centralized for CSPs with P-ATOs. However, at this time, the FedRAMP PMO does not have the resources to manage the assessment and authorization of all CSPs working with Federal Customers. Allowing for FedRAMP compliant Agency ATOs provides the flexibility needed for agencies to meet FedRAMP requirements.</p>
<p>As identified in the separate vuln management document, low vulns rarely indicate security weakness and should be eliminated from the report.</p>	<p>AO's should be aware of low vulnerabilities as an extreme number of low vulnerabilities could indicate possible risks or issues of concern. Lows are tracked, late lows are not.</p>
<p>For internal unremediated vulnerabilities details may be withheld for security purposes. Only the risk rating will be reported.</p>	<p>CSPs are required to report unremediated vulnerabilities for the system within the authorization boundary. If these unremediated vulnerabilities that are required for operations, then they should be reported as Operationally Required.</p>

Comment	Response
<p>Consistent with NIST SP 800-115, the initial rating assigned by the scanner is just a starting point for risk designation. The application of contextual factors is required by NIST guidance before arriving at a risk rating. This process is not an adjustment of risk rather a NIST specified process for determining risk.</p> <p>Tracking of the scanner suggested risk rating is not useful, does not bear context and thus overly burdensome. Only the final risk rating assigned by the CSP/3PAO should be reported and tracked</p>	<p>FedRAMP agrees with comment. Rating based on CVSS score is tracked. Analysis should be done to determine the actual risk level. However, this can be overly burdensome if done manually, so the deviation request process is used to adjust appropriately.</p>
<p>Scans do not provide an effective, complete illustration of a CSP’s risk posture. This data paired with POA&Ms metrics is not a sufficient basis ongoing authorization as it does not evaluate the effective implementation of relevant security controls.</p>	<p>Without direct access to the system, the use of POA&Ms and scans are the two of the factors that AOs need to consider in making an authorization decision.</p>
<p>Long term, review and authorization by the agencies and/or PMO is not scalable. Consider increasing accreditation and trust with 3PAO and move to an oversight position, especially for CSPs with a proven track record/level.</p>	<p>This document is more concerned with the current operations of FedRAMP. Comments on significant changes to the Continuous Monitoring process are out of scope for this document and should have been made in relation the "Evolution of FedRAMP Continuous Monitoring Framework" paper.</p>
<p>The frequency of deliverable should not be monthly as CSPs move within the multi-track model. The current scope of deliverables for continuous monitoring is a very small portion of a security program and not a good indicator of security.</p>	<p>FedRAMP currently requires the submission of monthly scans on POA&Ms.</p>
<p>The process as outlined in this document is not scalable for CSPs nor Agency or JAB authorizations. Consider increasing accreditation and trust with 3PAO and move to JAB to an oversight position, especially for CSPs with a proven track record/level.</p>	<p>This document is more concerned with the current operations of FedRAMP. Comments on significant changes to the Continuous Monitoring process are out of scope for this document and should have been made in relation the "Evolution of FedRAMP Continuous Monitoring Framework" paper.</p>

Comment	Response
<p>See above comment. Leverage 3PAO for monthly review to reduce AO/PMO review effort. Additionally the current frequency and scope of deliverables for continuous monitoring is a very small portion of a security program and does not provide a good indicator of security.</p>	<p>This document is more concerned with the current operations of FedRAMP. Comments on significant changes to the Continuous Monitoring process are out of scope for this document and should have been made in relation the "Evolution of FedRAMP Continuous Monitoring Framework" paper. FedRAMP currently requires the submission of Monthly scans on POA&Ms.</p>
<p>Remove reporting of detailed asset information. It is a liability to both the CSP and PMO to share this data. Asset lists or references should be obfuscated, for security purposes in limiting the exposure, and the 3PAO should review the obfuscation and key to ensure list is complete.</p>	<p>FedRAMP agrees that asset obfuscation is acceptable.</p>
<p>False Positives: If vulnerabilities are determined to be adjusted to a low risk due to operational requirement or it is a false positive AND the risk management process is relied upon, these should not need to be reported or considered a deviance. They should be treated like system identified low vulns.</p>	<p>False positives are only counted pending approval/verification by the AO. Once they are approved/verified, false positives are no longer counted. The government requests this information because the AO will want to see to see how risk levels were determined to make their own assessment.</p>
<p>Consider leveraging a 3PAO recommendation instead of requiring AO review, which can be redundant across agencies. 3PAO's have a much more intimate knowledge of the CSP environment and can best assess risk (initial and residual risk)</p>	<p>3PAOs and FedRAMP cannot assume risk for Federal Agencies, only the AO can assume risk and grant the authorization under Federal requirements.</p>

Comment	Response
<p>Rely on the CSP risk assessment model so that low vulnerabilities, false positives and pending operational risks do not need to be reported in either the monthly template or the POA&M template.</p>	<p>False positives and Operationally Required are only counted pending approval/verification by the AO. Once they are approved/verified, false positives and Operationally Required are no longer counted. AO's should be aware of low vulnerabilities as an extreme number of low vulnerabilities could indicate possible risks or issues of concern. The government requests this information because the AO will want to see to see how risk levels were determined to make their own assessment.</p>
<p>Again; AO review should be replaced with a simple review/acceptance of a 3PAO recommendation to reduce multiple agency reviews and the management of that effort.</p>	<p>3PAOs and FedRAMP cannot assume risk for Federal Agencies, only the AO can assume risk and grant the authorization under Federal requirements.</p>
<p>Low items and false positives should not be reported on the continuous monitoring template, this is duplicative of the POA&M. Due to the low value of this information and limited scope, it should not be reported twice.</p>	<p>The Continuous Monitoring template is an extraction/summary of the POA&M</p>
<p>3PAO's have a much more intimate knowledge of the CSP environment and can best assess advise in acceptance of risk, initial, and residual risk).</p>	<p>3PAOs and CSPs cannot assume risk for Federal Agencies, only the AO can assume risk and grant the authorization under Federal requirements.</p>
<p>The Raw Scanning Summary Graph plots the count of all instances of all unique vulnerabilities found in the automated scanning results. COMMENT: It is unnecessary and low value to have both graphs. Assessing the raw data and presenting the adjusted risks is the product of the CSP's security operations group. These processes are assessed during initial and annual assessments. Providing the raw data provides information that doesn't need to be processed by the govt and provides little value.</p>	<p>The FedRAMP JAB disagrees.</p>

Comment	Response
<p>This table should be struck. Final risk ratings are High, Medium or Low. Ratings assigned by the scanner are not a basis for “risk adjustment”.</p>	<p>The FedRAMP JAB disagrees.</p>
<p>Throughout its guidance, FedRAMP should clarify that any targeted remediation dates are calculated AFTER a suitable patch has been identified and tested by the CSP.</p>	<p>This comment is incorrect. CSPs are required to use the initial date of discovery of the finding in calculating the age of open POA&M items.</p>
<p>Additional clarification requested: Template includes the following two categories but the guide provides no additional guidance for the categories; Clarifiers for reviews And Considerations for trends. Please provide more detail about the expectations and intent of these items</p>	<p>This section is provided to allow the CSP to provide any additional details that may affect the AO's authorization decision or should be considered by the AO.</p>
<p>Additional clarification requested: The template identifies the following two categories of considerations: Deviation requests summary and Any irregularities in deliverables. See Deviation request notes above. For irregularities in deliverables, can you please provide more detail about the expectation and intent of this category. Providing examples would be helpful in this guide</p>	<p>This section is provided to allow the CSP to provide any additional details that may affect the AO's authorization decision or should be considered by the AO. Incident information should be included in the "Considerations for Review" section.</p>
<p>Additional clarification requested: The template adds the following detail to this section of the template: [Things the Authorizing Official’s (AO) team should be aware of regarding vendor, expected changes upcoming, new services, etc.] Does this section outline the significant changes/new services? Can more detail be provided about expectations and intent of this section? For instance, is it necessary to report 3PAO assessor change (individual)? How does risk posture of each CSP affect the type of information included here?</p>	<p>This section is provided to allow the CSP to provide any additional details that may affect the AO's authorization decision or should be considered by the AO. This may include things such as major changes.</p>

Comment	Response
<p>ID - Is there a naming convention issued by the PMO that will make cataloging consistent?</p>	<p>There is not an issued naming convention. If you are looking for suggestions, we suggest V-[incremented number]-[quarter] ex. V-123-3Q14</p>
<p>Other general comments: -Inventory tab should be eliminated. Inventory of assets should be obfuscated and full asset list/key should be reviewed by 3PAO</p>	<p>We require the same details as found on the SSP. You are free to obfuscate the asset details on the inventory tab, but you need a unique identifier of some kind, and the inventory must remain consistent with the scanner findings, and between months.</p>
<p>Asset Modifier - This level of asset detail should never be gathered. It should be obfuscated and the full asset list and key should be reviewed by the 3PAO</p>	<p>You are free to obfuscate the data as you see fit. This field is for a unique asset identifier; we had suggested using an IP address, but it is not necessary. The requirements are uniqueness and consistency</p>
<p>Status Date - The frequency of reporting should be based on the multi-track model. Monthly reports when no status change occurs simply creates noise.</p>	<p>There should always be some monthly status change, provided that actions are actually being taken to handle the item.</p>
<p>Original Risk Rating - An original risk rating infers it was automatically assigned by a scanner. Clarify how original risk rating should be approached when source is not from scanner.</p>	<p>The 3PAOs will provide a determination for the impact and risk for non-scanner items.</p>
<p>Also, while this is the Monthly ConMon Summary, the details solely focus on vulnerability scanning with no summarized details on Change Management or IR summaries. To clear up the ambiguities of the last two sections, could they not be an area to summarize the preceding month's activities in those two areas?</p>	<p>Incident information and proposed changes should be included in the "Considerations for Review" section.</p>
<p>Please remove the "System Status" field. This reporting summary does not collect the correct information to draw such conclusion.</p>	<p>Disagree. AOs make this determination based on a review of the monthly deliverables and a combination of number of vulnerabilities (especially high impact vulnerabilities), age of vulnerabilities, and information in items of note and considerations.</p>

Comment	Response
<p>Please include a very clear statement in the Continuous Monitoring Monthly Reporting Summary Guide that the information collected through monthly reporting will NOT be used for comparative purposes. The information is not suitable for comparison.</p>	<p>Disagree. The information is used by the AO as an indicator of risk or areas of concern.</p>
<p>It is not necessary to have both graphs. Assessing the raw data and presenting the adjusted risks is the product of the CSP's security operations group and that process is assessed during initial and annual assessments. Providing the raw data provides information that doesn't need to be processed by the govt</p>	<p>Disagree. The FedRAMP and Federal AOs need to see both graphs as indicators. These are high level summaries and provide AOs with an ability to raise flags for further review if needed.</p>
<p>[Deviation requests summary] - Comment Deviations that are due to operational requirement or other risk judgment made by the CSP should not require approval as the risk process has been assessed.</p>	<p>Only the AO can accept risk for the Agency, therefore the AO must approve Operationally Required risks or other no-remediated vulnerabilities.</p>

2. FEDRAMP CONTINUOUS MONITORING REPORTING AND POA&M TEMPLATE FAQ

Question	Response
<p>Table 2-1, Adjusted Risk Level Descriptions. Has guidance been provided on the threshold that would have to be met to justify a downgrade from High to Low? Presumably there would have to be countermeasures in place to detect and respond to inappropriate activity.</p>	<p>CVSS is required to be used a standard for rating the severity of vulnerabilities.</p>
<p>Section 3.3, Scanning Summaries. Are CSPs required to use the CVSS as a standard for rating the severity of vulnerabilities?</p>	<p>CVSS is required to be used a standard for rating the severity of vulnerabilities.</p>
<p>When CSPs deliver the monthly CM report, do they have to provide raw scan results and screenshots of the scan configuration?</p>	<p>Yes, CSPs are required to provide raw scan results and the information on the scan configuration.</p>
<p>Figure 3.1, Unique Scanning Summary a. How is the value for the “Annual” data points determined. Is it the total number of unique vulnerabilities carried over from the previous year or performed as part of an Annual Assessment?</p>	<p>The unique scanning summary contains a count of each unique vulnerability found in the automated scanning results. The annual date is based on the CSP's most recent annual assessment or the ATO date for recently authorized CSPs.</p>

Question	Response
<p>Page 10, Section 2.2 states addresses “vendor dependent risks.” We execute service contracts with multiple vendors, some of whom are not responsive to federal requirements, particularly in regards to PIV enabling their products. How are “vendor dependent” risks handled from a contract perspective? Because these risks “require action on the part of the product vendor,” will new clauses be added to the Federal Acquisition Regulation (FAR) to address non-complaint vendors? If a vendor does not mitigate these risks within the required 30 day timeframe, is that grounds for terminating a contract?</p>	<p>The FAR is not within the FedRAMP scope of operations. We can only suggest that Federal Agencies include terms and conditions in their contracts that would allow the Agency to terminate the contract if the service level requirements are not met. We would expect that this sort of clause would be standard in most government contracts.</p>
<p>1) Deviation Request Form (DRF) template (Section 2.2) Does it still include Date Change? I’m pretty sure it still has Risk Adjustment (but that’s been omitted in doc section 2.2). Has Vendor Dependency been added? It would help to have the DRF template embedded in this Con Mon Reporting doc that’s being reviewed and to have the DRF template available on the FedRAMP web site with the other templates.</p> <p>2) Approval of Deviation Requests (Section 2.2.1) Explain the process. I suggest removing some info from this section that is duplicated later in the document.</p>	<p>1. FedRAMP is in the process of updating the deviation request form. At this time, we do not review date changes, as they are considered late regardless of the request.</p> <p>2. Risk adjustments and vendor dependencies should be included. Deviation requests are reviewed by the FedRAMP ISSO. Once the ISSO reviews and agrees, the request is then passed to the JAB for approval.</p>

Question	Response
<p>1) Scanning Summaries (Section 3.3) How do the graphs get produced? Will FedRAMP be providing CSPs with a tool to produce those graphs?</p> <p>2) Risk Adjustment POA&M Item Counts (Sections 3.5.1 and 3.5.2) Would a High OR obtain AO approval? Or must the OR be mitigated as a High/Mod to reduce risk before AO approval will be granted for that item representing a lingering risk? (See 2nd paragraph in the “Operationally Required Vulnerabilities” section.)</p> <p>3)When can items be moved to the “Closed POAM Items” tab? Must old closed/completed/green items be translated into new column format? Or can those just be moved to the “Closed POAM Items tab “ in their old column format to save time on items that are historic, not recent and current</p>	<p>1. The CSP is expected to produce the graphs. FedRAMP does not provide a tool as these graphs can be produced in a number of widely available programs such as MS Excel.</p> <p>2. A high OR must be remediated to a moderate risk level before it can be accepted by the AO. An unremediated high OR that is older than 30 days is considered past due.</p> <p>3. We will assist in the first month’s closed tab; leave off historical closed items for the time being. In the future it will be necessary when tracking a CSPs ability to close items in the proper amount of time.</p>
<p>3.4. Open POA&M Summary</p> <p>1. The tables’ column headers show by quarter (Dec, Mar, Jun), not by month. Which is the intended timeframe?</p> <p>2. How does AO provide final approval for closure? I don’t think that’s via DRF. We’ll want record of which have been approved vs. which are pending approval. What is the trigger that allows CSP to move closed items to the “Closed POAM Items” tab of the POA&M spreadsheet?</p>	<p>1. FedRAMP will update the column headers to display reporting by month.</p> <p>2. FedRAMP has a process for approving final closure with the JAB; however, Agencies will have a slightly different process. This document provides a high level overview to account for both situations.</p>

Question	Response
<p>Will this document mean that the current Attestation Document due at initial Authorization will no longer be necessary</p>	<p>FedRAMP is no longer using the Self-Attestation template.</p>
<p>Does it [Operationally Required (OR)] mean that the vulnerability exists because if it didn't the platform could not operate? You should say what the definition of "Operationally Required" means.</p>	<p>Operationally Required (OR) exist only for vulnerabilities where the ability to remediate a vulnerability does not exist or remediating the vulnerability will cause failure of the CSP's service.</p>
<p>What is the impact of this? How long can something be overdue before it is a significant problem? If a CSP keeps making date adjustments, there must be some point where this is considered to be a deviation request. Without making it a deviation request, it is possible for a risk to "fly under the radar" for some period of time?</p>	<p>POA&Ms are tracked from the date of discovery. The CSP cannot simply continue to push back the remediation date. High POA&M items must be remediated in 30 days and moderate must be remediated in 90 days. Late POA&Ms are considered a significant risk and may trigger a review of the CSP's ATO/ P-ATO.</p>
<p>Just because the CSP is talking to the vendor doesn't mean that the vulnerability doesn't pose a risk. What is the impact of "past due"? How long can something be "past due" before it is considered an issue?</p>	<p>We do understand that vendor dependencies to pose a risk. We also understand that the remediation of this vulnerability is generally out of the hands of the CSP (for example a vulnerability in an OS that must be patched by Microsoft. Any high vendor dependencies must be lowered to moderate in 30 days. We are currently developing guidance for CSPs' that consistently show a pattern of past due POA&Ms and establishes indicators which may trigger a review of their ATO/P-ATO.</p>

Question	Response
Do we need to draft these (Deviation Request) in a risk acceptance memos? How do we document these?	FedRAMP will consider adding the Deviation Request Form to the POA&M Summary Guide.
Where should the CSP/CTS document the false-positives so that the next scan they can ignore those?	CSPs can manage False Positives as they see fit. However, when the AO sees an approved false positive on a scan, it will not be included in the POA&M.
This is for downgrading the risk. What if we need to upgrade the risk based on the no. of instances of the same finding in the environment?	The process is similar for downgrading and upgrading risks. FedRAMP will add additional language to clarify this process.
Do the accepted risks (vendor related and overall cloud- related have to have timelines or are they just accepted)? - The risk should be re-looked at from time to time and not be a permanent risk acceptance. A timeline should be defined here.	Vendor dependencies must be remediated within 30 days or the release of a patch or fix. High vendor dependencies must also be remediated to a moderate within 30 days. Operationally Required vulnerabilities are an accepted risk within the system, but must be approved by the AO.
"A summary of these monthly deliverables in the Continuous Monitoring Monthly Reporting Summary must be made available to Authorizing Officials (AOs) who examine the reports to ensure the CSP is maintaining an appropriate risk posture that supports an authorization." Would this be made to agencies that are subscribed to that CSP through FedRAMP for review as well? Or only to "AOs"? Which "AOs" is this specifically speaking to (JAB and/or Agencies)? Specify for clarity. - As part of CM for each Agency to ensure their data is properly protected and CSPs are performing according to FedRAMP guidelines, it is good to have other Agencies be a third party reviewer (fresh set of eyes) of these deliverables to ensure that CSPs are abiding to the FedRAMP guidelines.	The JAB is the AO for FedRAMP P-ATOs. The continuous monitoring documents for CSPs with a P-ATO are stored in the FedRAMP Secure repository. Any Federal agency can request access to the CSP's security package and continuous monitoring documents. Agencies that have issued a FedRAMP compliant ATO to a CSP will need to work with the CSP to receive their continuous monitoring deliverables and data.

Question	Response
<p>Is there any kind of sanction/penalty if CSPs submit information that is not in accordance to FedRAMP guidelines, i.e., the ATO gets taken away until it gets re-assessed?</p>	<p>CSPs that do not meet FedRAMP requirements may trigger a review of their FedRAMP compliant ATO or P-ATO.</p>
<p>The basis of CDM is seeing risk near real time and in the "Evolution of FedRAMP" document, it had indicated that this was what FedRAMP is moving toward, but it seems the "CM Monthly Reporting Summary" is still focused on a monthly deliverable, vice every 72 hours (ideal). What about giving FedRAMP reviewers the access into the CSP reporting system/dashboard (which means CSP must have CDM implemented). - Just a general observation. It is understood that this is difficult but to move toward CDM, this should be considered for each CSP.</p>	<p>This document is more concerned with the current operations of FedRAMP. Use of a CDM dash board is something that FedRAMP may consider in the near future.</p>
<p>This section only identifies the problem, but no action that is required out of the CSP. If a POAM is past due, what does FedRAMP do to enforce the CSP to comply? - This section is merely an "FYI" and does not hold any kind of value for AOs and subscribed agencies.</p>	<p>CSPs must meet FedRAMP requirements to maintain their P-ATO. A CSP that repeatedly fails to meet these requirements may have their ATO revoked. The guide does not address this issue as it mainly describes how to assemble the POA&M summary report.</p>
<p>"If the vulnerability cannot be remediated within 30 days, vendor dependencies at a high risk level must be mitigated to a moderate impact level by the CSP within 30 days" - this doesn't make sense? - Clarify</p>	<p>Here is an example to answer your question: If the CSP is waiting for a vendor to provide a patch to fix a high vulnerability, if that vendor cannot or does not provide the patch in 30 days, the CSP must implement an alternative measure to bring that vulnerability down to a moderate level until the vendor sends the patch.</p>

Question	Response
<p>What happens when a vendor state that there is no plan to fix the vulnerability and/or they do not consider the vulnerability significant enough to warrant any change and/or its part of their design? - Action from the CSP should be taken to 1. look for another vendor/product, 2. submit request for risk acceptance by the JAB (if 1 cannot be done), and 3. continuous follow up with vendor to see if they will change their tune to fix the weakness.</p>	<p>The CSP manages the system with vendor dependencies included. The AO may choose to accept the vendor dependencies or not. Open vendor dependencies require a minimum of monthly status updates (CSPs reaching out to the vendor for status) to not be considered late.</p>
<p>If the AO makes this determination on what the risk level is, why is it on the template that a CSP would have to complete? - if given the choice, the CSP would always give themselves a "green" status. If the AO make the determination, there should be a separate document or attachment to this document for AO review/feedback with an acceptable risk level and signatures by the AOs.</p>	<p>As noted in the guide, "AOs make this determination based on a review of the monthly deliverables and a combination of number of vulnerabilities (especially high impact vulnerabilities), age of vulnerabilities, and information in items of note and considerations. This section in the summary is included for the AO's use.</p>
<p>Who determines whether the original vulnerability is High, Mod or Low? Is this predetermined by the scanners or by the CSP? - For better clarification and impartiality</p>	<p>Most scanners use the CVSS standard as the default determination of the vulnerability's risk level.</p>
<p>What is the threshold for LOW POA&Ms? There's no explanation and not sure if Chart is clear to show that anything past 121 days is past due for Low POAMs? - Clarify so all audience can understand. -- Found in 3.6.1 that it is CSP defined. This means that CSP may *never* close out Low POA&Ms? This could be an issue for specific subscribed Agency AO.</p>	<p>Late Low POA&Ms are not tracked. However, FedRAMP's general guidance is that lows are expected to be addressed either within the next annual assessment cycle or 6 months, whichever is greater.</p>

Question	Response
<p>Is there a requirement for CSPs to comply to penetration testing at any given time? Or is this only done when they are due for a new ATO? If that is the case, what about when it moves to OA? - Using automated tools are great but there are also vulnerabilities that are found via manual testing or manual testing can determine that the risk associated with the vulnerability should be higher than the predetermined value due to the information (or amount of information) that can be divulged from the vulnerability.</p>	<p>FedRAMP requires CSPs to have a 3PAO perform announced penetration testing at least annually or when there is a major significant change to ensure compliance with all vulnerability mitigation procedures. The requirement for penetration testing does not exclude other methods of assessing other controls.</p>
<p>“Summary information is requested from CSPs in order to provide easier analysis of the continuous monitoring reporting.”</p> <p>Need to determine if summary information is a one-time snapshot or the average of the multiple scans for the time period, that is, would it be a monthly scan or the average of the collection of scans every 3 days for that month, etc.?</p>	<p>This summary information provides a one-time snapshot.</p>
<p>“If an AO needs to review full copies of vulnerability scans, updated POA&Ms and updated inventories, in order to validate, interpret, or make decisions based on information contained in the report, these documents should be made available by the CSP.”</p> <p>Is it to validate or to understand and make decisions about?</p>	<p>Full copies of the POA&Ms and scans are made available to the AO to ensure the AO can review the raw results or the complete document to gain a more in-depth understanding of the system's risk posture.</p>

Question	Response
<p>“Past due POA&M items represent risks to AOs. This is interpreted as an inability of CSP to meet the FedRAMP requirements and potentially identifies key risks that AOs should be aware of. Also, a repeated history of past due POA&Ms in and of itself can be a key indicator of risk and may indicate misaligned priorities between business processes and operations within a CSP.”</p> <p>Is this an accurate description? If every scan finding, even low risk items, must be reported and every unique vulnerability requires a POA&M (both of which are stated in this document), then all past due POA&M items may not represent a key risk.</p>	<p>FedRAMP places more emphasis on the CSP's ability to remediate moderate and high POA&Ms. Late high and moderate POA&Ms may indicate risks or an issue that could concern the AO. While low POA&Ms don't have a specific remediation date, an extremely high level of late, unremediated low POA&Ms could also indicate risks or issues that may concern the AO. FedRAMP does recognize that certain risks may be more important to the AO based on their risk tolerance.</p>
<p>“The Unique Scanning Summary graph provides a count of each unique vulnerability found in the automated scanning results. Each unique vulnerability identifier (as identified by the scanner) is only counted once.”</p> <p>It would appear that there is a translation from vulnerabilities that are IT asset specific to an external function (application usage) view point. It is not clear that this is a fully inclusive set (DB, Web, OS).</p>	<p>The Web, OS and DB scans are broken out in the unique scanning summary.</p>
<p>Total POA&M Count Table:</p> <p>This seems to reflect that the CSP would be reporting all of their information in a collective report. What visibility would a Department/Agency have of their use of the CSP? Would/could the D/A be able to get reporting only on the items providing the services to them?</p>	<p>The reports of all CSPs are not consolidated into a single report. Each CSP would provide a report for their system only. The AO only sees the POA&Ms and reports for CSPs that provide services to the agency.</p>

Question	Response
<p>The monthly reporting summary template is already included in the Continuous Monitoring Strategy Guide from 6/6/14. How does this document related to the Guide? Will the template in this document replace the one in the Guide?</p>	<p>This guide is intended to replace Appendix B in the “FedRAMP Continuous Monitoring Strategy and Guide.” The summary guide provides a high level view of the monthly POA&M submissions while the POA&M tracking sheet provides the details.</p>
<p>Need to understand how significant change requests are affiliated with monthly reporting</p>	<p>The CSP is required to submit major system changes and receive approval at least 30 days before implementing the change. Planned changes may affect the system's security posture and the AO may want to take this into consideration along with the review of the CSP's other monthly deliverables.</p>
<p>Deviation Requests - Additional clarification requested:</p>	<p>What type of clarification is needed? This comment is unclear.</p>
<p>The determination of status is more qualitative than quantitative and can vary between AO’s. Can more detail be provided via a standard methodology or guidance so status is quantitatively identified?</p>	<p>This guide does provide guidance of the review of the summary; however each agency’s level of risk acceptance is different.</p>
<p>Original Source Detector - Detection can occur from many sources, not just automated scanners. Is there guidance on how to record other sources?</p>	<p>We updated the template with an example of another document, but simply stating the document name is sufficient.</p>
<p>Milestone Changes - It is unclear where a change in completion date should be documented. Could we clarify how it's managed and where it's documented?</p>	<p>Typically the completion date does not change for items. The only cases where the completion date can be changed are with low vulnerabilities, and during a vendor dependency. These can be officiated with a “Completion Date Change Request Form”</p>
<p>Deviation Request ID - Is there a naming convention issued by the PMO that will make cataloging consistent?</p>	<p>There is not an issued naming convention. If you are looking for suggestions, we suggest D-[POAM ID]-[incremented number]-[quarter] ex. D-123-1-3Q14</p>

Question	Response
<p>Why is this document being classified as U//FOUO? This imposes specific distribution restrictions and since there are no details, is this simply intended to keep these details undiscoverable (i.e., FOIA)? Is there any specific guidance FedRAMP has on distribution and storage requirements?</p>	<p>For Official Use Only (FOUO) is a document designation, not a classification. This designation is used by Federal Agencies to identify information or material which, although unclassified, may not be appropriate for public release. The completed POA&M summary is appropriate for government but not public release.</p>
<p>The determination of status is more qualitative than quantitative and can vary between AO's. Can more detail be provided via formulas or guidance so status is quantitatively identified. Also, the POAM count is not identified as a status factor. Should it be?</p>	<p>This guide does provide guidance of the review of the summary; however each agency's level of risk acceptance is different. POA&M counts are included in the tables and identified as a status factor.</p>
<p>Further, the only thing I see the graph doing is breaking down the scans by target type (i.e., web, DB, OS); is there distinct agency reporting aligning with this graph? Otherwise, not sure what purpose that breakout serves.</p>	<p>The breakout serves to document why there are spikes every quarter. The FedRAMP updated for NIST SP 800-53 Rev. 4 requires every scan monthly.</p>
<p>[Clarifiers for reviews] - Comment: Please provide more detail about the expectations and intent of these items</p>	<p>This section is provided to allow the CSP to provide any additional details that may affect the AO's authorization decision or should be considered by the AO.</p>
<p>[Any irregularities in deliverables] - Comment For irregularities in deliverables, can you please provide more detail about the expectation and intent of this category? Providing examples would be helpful in this guide Significant change requests should be added here so the CSP can track AO approvals</p>	<p>This section is provided to allow the CSP to provide any additional details that may affect the AO's authorization decision or should be considered by the AO.</p>

Question	Response
<p>[Things the Authorizing Official’s (AO) team should be aware of regarding vendor, expected changes upcoming, new services, etc.] –</p> <p>Comment: Can more detail be provided about expectations and intent of this section? For instance, is it necessary to report 3PAO assessor change (individual)? How does risk posture of each CSP affect the type of information included here?</p>	<p>This section is provided to allow the CSP to provide any additional details that may affect the AO's authorization decision or should be considered by the AO.</p>